CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Statement of Deven McGraw

Director, Health Privacy Project

Center for Democracy & Technology

Before the

House Energy and Commerce Committee

on the

Discussion Draft of Health Information Technology and Privacy Legislation

June 4, 2008

Chairman Dingell, Ranking Member Barton, and members of the Committee, thank you for holding this hearing on the discussion draft of Health Information Technology and Privacy Legislation developed by the Chairman and Ranking Member of the Committee, and Chairman Pallone and Ranking Member Deal of the Subcommittee on Health.

CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works to keep the Internet open,

innovative and free by developing practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation. The Health Privacy Project, which has more than a decade of experience in advocating for the privacy and security of health information, was merged into CDT earlier this year to take advantage of CDT's long history of expertise on Internet and information privacy issues and to come up with workable solutions to better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

Just a couple of weeks ago, CDT released a comprehensive paper calling on Congress to enact – and all stakeholders to adopt - a comprehensive privacy and security framework to cover electronic health information. Some of the points raised in that paper are highlighted in this testimony today, but I also request that the full copy, which is attached and can be found at www.cdt.org/healthprivacy/20080514Hpframe.pdf, be entered into the hearing record.

The discussion draft takes critical steps toward that goal by setting forth incremental, workable privacy and security solutions that build on current law and target many of the key issues raised by the new e-health environment. CDT is pleased to support this draft, which will help increase public trust in health information technology and health information exchange and facilitate the movement of the nation to an interconnected, electronic health system.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and health information exchange can help improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. Survey data shows that Americans are well aware of both the benefits and the risks of health IT. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers – because they believe such access is likely to increase their quality of care. At the same time, people have significant concerns about the privacy of their medical records. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[1] In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information. [2]

[1] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005) (2005 National Consumer Survey).

[2] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

Health IT has a greater capacity to protect sensitive personal health information than is the case now with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.[3]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects underscore these concerns, and this is just one of numerous examples. The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a lack of enforcement of existing

[3] See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[4]

With rare exception, national efforts to advance greater use of health IT have not adequately or appropriately addressed the privacy and security issues raised by the movement to electronic health records. While some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT can bring, it is clear that the opposite is true: enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits.

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[5] Without appropriate protections for privacy and security in the healthcare system, patients will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[6] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[7] Persons who report that they are in fair or poor health

[4] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[5] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[6] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

[7] Harris Interactive Poll #27, March 2007.

and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.[8]

The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[9]

It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy.

[8] 2005 National Consumer Survey.

[9] Id.

We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

To build public trust in health IT, we need a comprehensive privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. In developing this comprehensive framework, policymakers, regulators, and developers of HIT systems need not start from scratch. A framework for HIT and health information exchange already exists, in the form of the generally accepted "fair information practices" ("FIPS") that have been used to shape policies governing uses of personal information in a variety of contexts, most notably the HIPAA Privacy Regulation, which established the first federal health privacy framework.[10] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's multi-stakeholder Connecting for Health initiative, would:

- Implement core privacy principles;
- Adopt trusted network design characteristics; and
- Establish oversight and accountability mechanisms.[11]

Congress should set the framework for national policy through legislation – but ensuring and enforcing adequate protections for privacy and security also will require coordinated actions on the part of key regulatory agencies, as well as industry best practices. The framework should be implemented in part by strengthening the HIPAA Privacy Rule for

---

[10] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

[11] See www.connectingforhealth.org for a more detailed description of the Common Framework.

records kept by the traditional health system participants, but also needs to address the increased migration of personal health information out of the traditional medical system.

As set forth in more detail below, we are pleased that this discussion draft addresses so many of the elements of fair information practices. The draft takes some critical steps forward in the effort to establish a framework of comprehensive privacy and security protections that will build consumer trust in health IT and help break the privacy "logjam" that has to date thwarted efforts to increase the federal investment in building an interoperable, nationwide electronic health system. We hope that this draft marks the beginning of a longer-term effort on the part of Congress and other policymakers to address privacy and security of health information as part of an overall conversation about how to move our health care system into the 21st Century.

Strengthening HIPAA Privacy and Security Rules to Meet New Challenges

The federal privacy and security rules that took effect in 2003 under the Health Insurance Portability and Accountability Act (HIPAA) reflect elements of a comprehensive framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. The HIPAA Privacy Rule was a landmark in privacy protection, but it is widely recognized that the regulation is insufficient to adequately cover the new and rapidly evolving e-health environment. This discussion draft includes important provisions to address these gaps. For example:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by the Privacy Rule. The discussion draft makes it clear that RHIOs, HIEs, E-prescribing Gateways must be business associates of covered entities in order to receive and exchange protected health information. The draft strengthens the protections for consumers whose information is maintained or accessed by business associates by making these entities directly accountable for meeting the HIPAA Security Rule Provisions and making them subject to the HIPAA civil or criminal penalties for failure to comply with those rules. The draft also makes it clear that business associates cannot access, use or disclose protected health information except in accordance with the provisions of their business associate contract and makes business associates directly accountable to federal authorities for any failure to comply with the data use provisions in these contracts. These provisions in the HIPAA regulations are fundamental tenets of good data stewardship, and anyone who touches this sensitive data should be accountable for complying with them.

- The discussion draft establishes a federal right to be notified in the event of breach by a covered entity or business associate of protected health information, if the unauthorized use of the information could reasonably result in substantial harm, embarrassment, inconvenience or unfairness to the individual. These provisions would establish for the first time a national right for consumers to at least be notified when the security of their health information is compromised.

We ask the supporters of this discussion draft to consider establishing a rebuttable presumption that encrypted information that is inappropriately accessed or disclosed is not subject to the notification requirements, which is the approach followed in the draft with respect to breach notification requirements for personal health record vendors.[12] Such an approach would create a powerful incentive for entities that hold personal health information to adopt strong encryption controls, thereby significantly minimizing the likelihood of data breach and consumer harm.

- As noted above in our testimony, more than 3/4 of consumers are concerned that their medical information will be used to market products or services back to them. We hear frequently from people who have received communications encouraging them to use specific drugs or other health care products or services that they are alarmed that someone must have accessed their medical information in order to target them with these communications. The HIPAA Privacy Rule already prohibits the use of protected health information for marketing purposes without a patient's express authorization. But the definition of marketing has been interpreted by some to permit, without authorization, "patient education" communications that consumers would clearly perceive to be marketing. The discussion draft closes that loophole by making it clear that a communication

[12] In the alternative, the bill could establish that unauthorized access to or disclosure of unencrypted information is the "trigger" for breach notification, instead of leaving it up to the subjective judgment of the entity holding the information about whether the breach would harm or be embarrassing or unfair to the individual.

must meet all three of the exemptions in the current Privacy Rule marketing definition in order to be exempt from the requirement of patient authorization.

- The HIPAA Privacy Rule gives patients the right to receive an "accounting" of certain disclosures of their health information – but this right does not apply to routine disclosures for treatment, payment or health care operations. Electronic technologies provide covered entities with the ability to easily track precisely who has accessed a patient's medical record, and we understand that most health care entities using electronic health records are already using these electronic "audit trails" to control who can access a patient's record and to track and monitor every touch of a patient's record. The discussion draft would require entities using these electronic tools to allow patients to receive a copy of that audit trail upon request. Few consumers are likely to take advantage of this right – but knowing it is possible to get a copy of who has accessed your medical records goes a long way to building consumer trust, and engages patients in the effort to ensure that information in their record is accurate, complete and current.

- The Privacy Rule gives patients the right to request a restriction on uses and disclosures of their information for treatment, payment and health care operations – but currently a covered entity is under no obligation to grant the request. The discussion draft makes it clear that in cases where a patient wants to pay for medical care out-of-pocket, a covered entity must honor a request to not disclose information related to that care to an insurer specifically for payment purposes.

We note that the draft still permits the covered entity to use and disclose information for treatment and health care operations, which includes a number of health care coverage functions that health insurers and plans have long claimed are critical to their business operations.

- A critical element of fair information practices is that data should be collected and used only for specific and appropriate purposes. The HIPAA Privacy Rule requires covered entities to request – and use and disclose – only the minimum amount of information necessary to accomplish their legitimate purposes, except when information is being used or disclosed for treatment purposes. The minimum necessary provisions are broadly worded and meant to be flexible to respond to the particular context. Unfortunately, covered entities often say that they are confused by the minimum necessary rule – and the frequent result misinterpretation of the law. The discussion draft clarifies this provision – and further protects patient privacy – by making it clear that for uses other than treatment, covered entities should use a limited data set when they use and disclose protected health information for routine purposes, except in cases where a limited data set would not accomplish the legitimate purpose for which the information is sought.

Establishing Privacy Protections for Personal Health Records

Personal health records and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers,

will not be covered by the HIPAA regulations unless they are being offered to consumers by covered entities. In this unregulated arena, consumer privacy will be protected only by the PHR offeror's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the Federal Trade Commission (FTC) may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.[13] The absence of any clear limits on how these entities can access, use and disclose information is alarming – and has motivated some to suggest extending the HIPAA Privacy Rule to cover PHRs. But we believe that the Privacy Rule, which was designed to set the parameters for use of information by traditional health care entities, would not provide adequate protection for PHRs and may do more harm than good in its current scope. Further, it may not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

We believe the discussion draft – which tasks HHS and FTC with jointly coming up with recommendations for privacy and security requirements, as well as breach notification provisions, for PHRs – proposes the right approach for ultimately establishing comprehensive privacy and security protections for consumers using these new health tools. For PHRs offered by entities that are not part of the traditional health care system,

---

[13] The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

it is critical that regulators understand the business model behind these products, which will largely rely on advertising revenue and partnerships with third-party suppliers of health-related products and services. Relying solely on consumer authorization for use of information shifts the burden of protecting privacy solely to the consumer and puts the bulk of the bargaining power on the side of the entity offering the PHR. For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – clear rules are needed regarding marketing and commercial uses that will better protect consumers. We are pleased that the discussion draft lays the foundation for the establishment of these rules, and tasks the FTC with enforcing breach notification provisions until these rules can be established.

Congress Should Also Consider Strengthening HIPAA Enforcement

When Congress in enacted HIPAA in 1996, they enacted civil and criminal penalties for failure to comply with the statute – and these penalties applied also to the subsequent privacy and security rules implemented years later. Unfortunately, the HIPAA rules have never been adequately enforced. The HHS Office for Civil Rights (OCR), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[14] The Justice Department has levied some penalties under the criminal provisions of the statute – but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limits the application of these criminal provisions to just

[14] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008) http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

covered entities, which has required prosecutors to bootstrap other legal provisions in order to criminally prosecute certain employees of covered entities who have criminally accessed, used or disclosed a patient's protected health information.[15]

The discussion draft requires HHS to annually report to Congress on enforcement of the HIPAA rules and establishes privacy officers in each HHS regional office, which are good first steps in securing better enforcement by both increasing Congressional scrutiny and raising the visibility of privacy as an HHS priority. But Congress should consider doing more, by either strengthening the provisions of the discussion draft as discussed below, or holding hearings on better enforcement of HIPAA and addressing the issue in subsequent legislation. A lax enforcement environment sends a message to entities that access, use and disclose protected health information that they don't have to devote significant resources to compliance with the rules. Without strong enforcement, even the strongest privacy and security protections are but an empty promise for consumers.

Congress should:

- Carefully examine the statutory enforcement provisions in HIPAA and consider whether amendments are needed to strengthen OCR and DOJ's authority to impose criminal or civil penalties (and at a minimum, making it clear that the penalties can be assessed against covered entities, business associates, *and their employees* for violations of HIPAA).
- Consider how individuals who are significantly harmed by misuse of their

[15] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences.

information can be made whole, or at least have access to meaningful recourse.

- Consider expressly authorizing state authorities (such as the attorneys general) to also enforce HIPAA.
- Consider establishing penalties for the re-identification of de-identified data.

Other Good Provisions of the Discussion Draft

- While the Privacy Rule includes criteria for de-identifying data, these criteria are now five years old – and new technologies and the increased availability of data on-line may be making it much easier to re-identify once de-identified health information. We are pleased that the discussion draft tasks HHS with coming up with guidance on how best to implement the HIPAA privacy rule requirements on deidentification, providing an opportunity for an update to these provisions.

- We praise the discussion draft for authorizing $10 million for a comprehensive national education initiative to enhance public transparency regarding uses of health information and the effects of such uses.

- We also endorse the provisions calling for a GAO report on best practices related to disclosure among health care providers of protected health information for treatment purposes, as well as those that make it clear that stronger state privacy rules are preserved, which has always been an important component of HIPAA.

- We also believe the discussion draft sets up an administrative infrastructure for moving health IT forward that is better than what exists currently (or has been

proposed by the administration), and what is currently being considered in the Senate. In the draft, the Office of the National Coordinator (ONC) is firmly established in statute and specifically tasked to develop and execute a strategic health IT plan, with specific objectives, milestones, and metrics for facilitating electronic health records and health information exchange, including the incorporation of privacy considerations and security protections. ONC also must specify a framework for coordination and flow of recommendations and policies among the various administrative agencies involved in health IT, as well as the two federal advisory bodies established in the discussion draft. The draft establishes a Policy Committee, which must be accountable to the public and recommend a policy framework for the development and adoption of health IT, and any recommendations for technology standards must flow from these policy recommendations, which is the appropriate way to make policy governing health IT and health information exchange.

The Appropriate Role of Consumer Consent

Recently, public debates about how best to protect the confidentiality, privacy and security of health information have focused almost exclusively on whether patients should be asked to authorize all uses of their health information. The ability of individuals to have some control over their personal health information is important, and a comprehensive privacy and security framework should address patient consent.[16] A

[16] Much more should be done to improve the way in which consent options are presented to consumers in the healthcare context. Internet technology can help in this regard, making it easier to present short notices, layered notices and more granular forms of consent.

number of states have passed laws requiring patient authorization to access, use and disclose certain sensitive categories of health information, and federal law prohibits the disclosure of substance abuse treatment records without express patient authorization. HIPAA Privacy Rules currently prohibit the use of certain types of information, such as psychotherapy notes, or prohibit use of information for certain purposes, such as marketing, without express patient authorization, and the Rules provide individuals with the right to object to certain uses and disclosures (such as in facility directories or to family members). The discussion draft provides consumers with a right to restrict the disclosure of their health information to insurers for payment purposes where they are paying out-of-pocket for a health care product or service. Health information systems must be structured in a way that allows these consents to honored and appropriately and securely managed.

But patient authorization is not a panacea, and as appealing as it may appear to be in concept, in practice reliance on consent would provide weak protection for consumer's health information. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is less protective of privacy and confidentiality.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated

decisions about use of their health data. Most don't read the details of a consent form and those that do often do not understand the terms. Many wrongly assume that the existence of a "privacy policy" means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[17] If mere patient authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are completely outside the scope of the HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if reliance on consent by an individual for any particular use of his or her information is treated by policymakers as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.[18]

The discussion draft provides better protections for consumer's health information by addressing who can access, use, and disclose protected health information and for what purposes, and ensuring that these rules are applicable to and can be enforced against both covered entities and business associates; by providing for notification in the event of

---

[17] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K. Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

[18] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

breach; by requiring entities using electronic health records to provide consumers with an audit trail upon request; by giving consumers a right to restrict use of their data for payment purposes when they choose to pay out of pocket; by placing parameters around minimum necessary and making it clear that a limited data set should be used unless more identifiable information is legitimately needed; by tasking HHS and FTC to come up with recommendations for appropriate rules to protect consumers using PHRs; and by calling for an assessment by HHS regarding the criteria for deidentification of data need to be updated.

Conclusion

Thank you for the opportunity to present this testimony in support of the discussion draft, which we believe moves us significantly closer to securing comprehensive, workable privacy and security protections for electronic health information systems. I would be pleased to answer any questions you may have.

Attachment

Summary – Testimony of Deven McGraw, Center for Democracy & Technology
Hearing on Discussion Draft of Health IT and Privacy Legislation

- Health information technology (health IT) and health information exchange can improve health care quality and efficiency. But consumers have concerns about the privacy of their medical information on-line. Health IT has greater capacity to protect privacy – but the movement of health information on-line also magnifies the risks.

- The failure to address these risks deepens consumer distrust in e-health systems. Enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT.

- We need a comprehensive privacy and security framework that is based on fair information practices (i.e., the Markle Foundation Common Framework) and sets clear guidelines for use and disclosure of electronic health information. The framework should build on HIPAA and incorporate protections for health information held by non-health care entities.

- CDT supports the discussion draft, which takes critical steps toward establishing this comprehensive framework. In particular, CDT supports:
  - Clarifying that health information exchanges are business associates, and making business associates directly accountable for complying with the HIPAA Security Rules and the data use requirements in their business associate contracts;
  - Establishing a right of consumers to be notified in the event of a breach (CDT asks the Committee to consider creating a rebuttable presumption that notification is not necessary if the data that is breached is encrypted);
  - Clarifying the definition of marketing in the HIPAA Privacy Rule;
  - Giving patients the right to receive an audit trail from entities using electronic health records;
  - Granting patients the right to restrict disclosure of their information for payment purposes when they are paying out-of-pocket;
  - Requiring the use of a limited data set for non-treatment purposes, except when doing so would not be feasible.
  - Tasking HHS and FTC with coming up with recommendations for privacy protections for consumers using PHRs, and tasking FTC with enforcing breach notification provisions in the interim.
  - Requiring HHS to come up with guidance on de-identification.

- The Committee should consider doing more – either in this draft or in future efforts – to strengthen HIPAA enforcement.

- There is an appropriate role for consumer consent in e-health systems, and those systems should be required to honor those consents when they are sought (either to comply with law or voluntarily). But requiring authorization for all data uses provides weak protection for consumers. The approach in the discussion draft moves us further toward securing comprehensive, workable privacy and security protections for electronic health information systems.

Comprehensive Privacy and Security: Critical for Health Information Technology

Version 1.0 – May 2008

In this paper, CDT calls for the adoption of a comprehensive privacy and security framework for protection of health data as information technology is increasingly used to support exchange of medical records and other health information. CDT believes that privacy and security protections will build public trust, which is crucial if the benefits of health IT are to be realized. In CDT's view, implementation of a comprehensive privacy and security framework will require a mix of legislative action, regulation and industry commitment and must take into account the complexity of the evolving health exchange environment.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and health information exchange can help improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. At the federal and state levels, policymakers are pushing initiatives to move the health care system more rapidly into the digital age.

However, health IT initiatives pose heightened risks to privacy. Recent breaches of health information underscore that the risks are real. At the same time, there is widespread confusion and misinterpretation about the scope of current health privacy laws. Some are pushing for quick "fixes" to try to address the public's privacy concerns, but fully resolving these issues requires a comprehensive, thoughtful and flexible approach.

While some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT can bring, it is clear that the opposite is true: enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits.

Survey data shows that Americans are well aware of both the benefits and the risks of health IT. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers – because they believe such access is likely to increase their quality of care. At the same time, people have significant concerns about the privacy of their medical records. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[19] In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

[19] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005) (2005 National Consumer Survey).

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 53% were concerned about insurers gaining access to this information. [20]

Appropriate privacy protections must be incorporated from the outset in the design of new health IT systems and policies. It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy. As an Internet policy organization and privacy advocate, CDT brings a unique perspective to these issues, based on our experience in shaping workable privacy solutions for a networked environment. In this paper, we describe why it is necessary that all parties—from traditional health care entities and new developers of personal health records, to legislators and regulators—address privacy and security in health IT systems. We emphasize that all stakeholders need to begin immediately to implement and enforce a comprehensive privacy and security framework in all of the various tools and processes of health IT.

The Consequences of Failing to Act

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information. [21] Without appropriate protections for privacy and security in the healthcare system, patients will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[22] According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[23] Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.[24]

---

[20] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

[21] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[22] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

[23] Harris Interactive Poll #27, March 2007.

[24] 2005 National Consumer Survey.

People who engage in privacy-protective behaviors to shield themselves from stigma or discrimination often pay out-of-pocket for their care; ask doctors to fudge a diagnosis; switch doctors frequently to avoid having all of their records in one location; lie; or even avoid seeking care altogether.[25] The consequences are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[26]

Health IT Can Protect Privacy – But Magnifies Risks

Health IT has a greater capacity to protect sensitive personal health information than is the case now with paper records. For example, it is often impossible to tell whether someone has inappropriately accessed a paper record. By contrast, technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing for appropriate purposes without needing to create large, centralized databases of sensitive information that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.[27]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects, and the accidental posting of identifiable

---

[25] Protecting Privacy; 2005 National Consumer Survey; Promoting Health/Protecting Privacy.

[26] Id.

[27] See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

health information on the Internet by a health plan, underscore these concerns, and are just two of numerous examples. The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with the lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[28]

Elements of a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

A comprehensive privacy and security framework must be implemented by all stakeholders engaged in e-health efforts. Such a framework, as outlined by the Markle Foundation's Connecting for Health, would:

- Implement core privacy principles;
- Adopt trusted network design characteristics;
- Establish oversight and accountability mechanisms.

Congress should set the framework for national policy through legislation. Ensuring and enforcing adequate protections for privacy and security also will require coordinated actions on the part of key regulatory agencies, as well as industry best practices. The framework should be implemented in part by strengthening the HIPAA Privacy Regulation for records kept by the traditional health system participants, but also needs to address the increased migration of personal health information out of the traditional medical system.

Notwithstanding the urgent need to address privacy, health information policy initiatives - both legislative and administrative – are moving forward without addressing privacy and security at all, or they are taking a piecemeal approach that too narrowly focuses on a single activity, such as e-prescribing, or on just one aspect of fair information practices, such as the appropriate role of patient consent.

In developing a comprehensive framework, policymakers, regulators, and developers of HIT systems need not start from scratch. A framework for HIT and health information exchange already exists, in the form of the generally accepted "fair information practices" ("FIPS") that have been used to shape policies governing uses of personal information in a variety of contexts, most notably the HIPAA Privacy Regulation, which established the first federal health privacy framework.[29] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle

[28] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[29] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

Foundation's Connecting for Health initiative, which includes broad representation from across the health care industry and patient advocacy organizations, describes the principles as follows:

- Openness and Transparency: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

- Purpose Specification and Minimization: The purposes for which personal data is collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

- Collection Limitation: Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

- Use Limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

- Individual Participation and Control:
    - Individuals should control access to their personal health information:
        - Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
    - Individuals should have the right to:
        - Have personal data relating to them communicated within a reasonable time (at an affordable change, if any), and in a form that is readily understandable;
        - Be given reasons if a request (as described above) is denied, and to be able to challenge such a denial:
        - Challenge data relating to them and have it rectified, completed, or amended.

- Data Integrity and Quality: All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete and current.

- Security Safeguards and Controls: Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

- Accountability and Oversight: Entities in control of personal health data must

be held accountable for implementing these information practices.

- Remedies: Legal and financial remedies must exist to address any security breaches or privacy violations.

The Connecting for Health Common Framework also sets forth characteristics for network design that can help ensure health information privacy and security.[30] These network design characteristics facilitate health information exchange not through centralization of data but rather through a "network of networks." Such a distributed architecture is more likely to protect information. Other key elements of such a system are interoperability and flexibility, which support innovation and create opportunities for new entrants.

The Role of HIPAA in the New Environment

The federal privacy and security rules that took effect in 2003 under the Health Insurance Portability and Accountability Act (HIPAA) reflect elements of this framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. The HIPAA Privacy Rule was a landmark in privacy protection, but it is widely recognized that the regulation is insufficient to adequately cover the new and rapidly evolving e-health environment. For example:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by HIPAA's Privacy Rule.

- Personal health records and other consumer access services now being created by third parties, including companies such as Google and Microsoft, as well as by employers usually fall outside of the HIPAA rules.

- Personal health data is migrating onto the Internet through an exploding array of health information sites, online support groups, and other on-line health tools, regulated only through enforcement by the Federal Trade Commission (FTC) of the general prohibition against unfair and deceptive trade practices, such as a failure to follow promised privacy policies.

- While the Privacy Rule includes criteria for de-identifying data, new technologies are making it much easier to re-identify once de-identified health information and to combine it with personal information in other databases, making it more likely

[30] See www.connectingforhealth.org for more details on the Common Framework.

that sensitive health information will be available to unauthorized recipients for uses that have nothing to do with treatment or payment.

In addition, the HIPAA rules have never been adequately enforced. The HHS Office for Civil Rights (OCR), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[31] Historically, states have filled the gaps in federal health privacy laws by enacting legislation that provides stronger privacy and security protections for sensitive data, such as mental health and genetic information. The states continue to have an important role to play, but relying on the states to fill deficiencies in HIPAA's Privacy Rule – or to regulate entities outside of the traditional healthcare sphere – does not provide a comprehensive, baseline solution that gives all Americans adequate privacy and security protections, and does not offer all the entities in the e-health space a predictable and consistent policy environment.

◪ National Conversations about Privacy and Security Have Been Too Focused on the Issue of Individual Consent

The ability of individuals to have some control over their personal health information is important, and a comprehensive privacy and security framework should address patient consent.[32] However, consent is not a panacea. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is less protective of privacy and confidentiality.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated decisions about use of their health data. Most don't read the details of a consent form and those that do often do not understand the terms. Many wrongly assume that the existence of a "privacy policy" means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[33] If mere patient

---

[31] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008) http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

[32] Much more should be done to improve the way in which consent options are presented to consumers in the healthcare context. Internet technology can help in this regard, making it easier to present short notices, layered notices and more granular forms of consent.

[33] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K.

authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are completely outside the scope of the HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if reliance on consent by an individual for any particular use of his or her information is treated by policymakers as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.[34]

All Entities Should Adopt and Implement a Comprehensive Privacy and Security Framework

Regardless of whether or not Congress takes action to address these issues, states and entities developing health information exchanges and other health IT initiatives should commit to adoption of the comprehensive privacy framework outlined here. Guidance for policy development for health information exchanges can be found, for example, in the Common Framework developed by the Markle Foundation's Connecting for Health Project. Consumer access services such as PHRs must also implement the comprehensive framework through rigorous privacy and security protections.[35] Such entities should make their privacy commitment explicit in a published privacy notice. Consumers should look for these promises and should measure them against the framework. Once companies make a privacy promise, they will be bound to it under the Federal Trade Commission Act. In addition, consumer rating services can compare and assess privacy practices, measuring them against the principles outlined here.

Congress Should Establish a Comprehensive Health Privacy and Security Approach

Although states and the private sector should not wait for action by Congress to protect privacy, CDT believes that Congress should establish national policy to ensure that health information technology and electronic health information exchange is facilitated by strong and enforceable privacy and security protections.

Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

[34] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

[35]See, e.g. the Best Practices for Employers offering PHRs http://cdt.org/healthprivacy/20071218Best_Practices.pdf.

According to recent surveys:

- 75% believe the government has a role in establishing rules to protect the privacy and confidentiality of online health information;
- 66% say the government has a role in establishing the rules by which businesses and other third parties can have access to personal health information; and
- 69% say the government has a role in encouraging doctors and hospitals to make their personal health information available over the Internet in a secure way.[36]

One of the major challenges in developing a comprehensive privacy and security framework is to integrate any new rules with the HIPAA privacy and security rules. Congress should consider both strengthening HIPAA where appropriate and establishing additional legal protections to reach new actors in the e-health environment. Congress should set the general rules – the attributes that a trusted health information system must have – based on the Fair Information Practices discussed earlier. Further, Congress should hold a series of hearings on some of the more difficult issues to resolve and develop a full record that will serve as the basis for more specific legislative action. In particular, Congress should consider:

- The appropriate role for patient consent for different e-health activities;
- The ability of consumers to have understandable information about where and how their Personal Health Information (PHI) is accessed, used, disclosed and stored;
- The right of individuals to view all PHI that is collected about them and be able to correct or remove data that is not timely, accurate, relevant, or complete;
- Limits on the collection, use, disclosure and retention of PHI;
- Requirements with respect to data quality;
- Reasonable security safeguards given advances in affordable security technology;
- Use of PHI for marketing;
- Other secondary uses (or "reuses") of health information;
- Responsibilities of "downstream" users of PHI;
- Accountability for complying with rules and policies governing access, use, and disclosure, enforcement, and remedies for privacy violations or security breaches;[37] and
- Uses and safeguards for de-identified information.

---

[36] 2006 Markle Foundation Survey.

[37] See the Common Framework, www.connectingforhealth.org.

◪ Congress Also Should Enact Legislation to Strengthen HIPAA For Health System Entities

With respect to the access, use and disclosure of electronic health information by the traditional players in the health care system, there are some immediate steps Congress could take to fill some of the gaps in HIPAA. For example, Congress can take a number of actions to secure more meaningful enforcement of the HIPAA rules, including:

- Strengthening Office for Civil Right's (OCR's) role by requiring it to conduct periodic audits of covered entities and their business associates to ensure compliance with the rules;
- Increasing the penalties associated with failure to comply with key provisions of the HIPAA rules;
- Increasing resources dedicated to HIPAA enforcement;
- Requiring OCR to report to Congress on a regular basis on enforcement of the rules; and
- Amending HIPAA to allow for enforcement of the rule by state authorities (such as attorneys general).

Congress should also consider enacting legislative provisions to:

- Establish notification requirements and penalties for data breaches;
- Strengthen the existing HIPAA rules requiring express authorization for use of patient identifiable data for marketing; and
- Require electronic health systems to provide consumers with access to their health information in an electronic format.

Although it is desirable for Congress to enact legislation that fills some of the gaps in HIPAA and to enact a general privacy and security framework to govern health IT, it will be impossible for Congress to legislatively adopt comprehensive rules that fit all of the various actors and business models in the rapidly expanding and evolving e-health environment. Therefore, a second major challenge for Congress is to decide what can be legislated and what must be delegated to agency rulemaking – and what areas are best left to be developed and enforced through industry best practices.

◪ Strengthening Privacy and Security Will Also Require a More Tailored Regulatory Approach

While Congress should establish a strong framework for health privacy and security, it must avoid a "one size fits all" approach that treats all actors that hold personal health information the same. The complexity and diversity of entities connected through health information exchange, and their very different roles and different relationships to consumers, require precisely tailored policy solutions that are context and role-based and flexible enough to both encourage and respond to innovation. For example, it makes little sense to have the same set of rules for "personal health records," which are often

created by and controlled by patients and held by third party data stewards outside the healthcare system, and for "electronic health records," which are created and controlled by health care providers for purposes of treatment and care management. To take another example, rules for use of personal health information for treatment need to be quite different than rules for marketing or other secondary uses. Rules regarding use of health information for research need to be separately considered as well.

Congress should not attempt to develop all of the details in legislation. Rather, Congress should enact legislation specifically recognizing the importance of the privacy rights in health information across technology platforms and business models, setting out principles and attributes to guide one or more regulatory agencies in developing detailed, context-specific rules for the range of entities that collect, use and distribute personal health information in the new interconnected healthcare system. One approach would be to direct the Department of Health and Human Services to strengthen the HIPAA regulations that apply to traditional players in the health system, while also directing HHS or possibly the Federal Trade Commission to issue regulations to govern the handling of personal health information by new players who are part of the broader Internet marketplace and not part of the healthcare system. If more than one agency is to be involved, Congress could require them to work together to avoid issuing conflicting rules (as the financial services regulatory agencies did in developing security rules for financial information).

Tasking HHS and/or the FTC with the responsibility for developing detailed regulations allows for:

- A more tailored, flexible approach that will ensure comprehensive privacy and security protections in a myriad of different e-health environments, and
- More regular, active monitoring of developments in the marketplace and a more rapid response to newly emerging privacy and security issues.

Congress should maintain strong oversight over the regulatory process by:

- Requiring regulations to be developed within a particular timeframe;
- Requiring satisfactory completion of the rulemaking before federal HIT grants can be made;
- Mandating reporting by the agencies on implementation and enforcement; and
- Vigorous oversight and reporting on implementation and enforcement.

Conclusion

To establish greater public trust in HIT and health information exchange systems, and thereby facilitate adoption of these new technologies, a comprehensive privacy and security framework must be in place. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. Congress should set the framework for privacy and security by strengthening enforcement of existing law and ensuring that all holders of personal health

information are subject to a comprehensive privacy framework. Congress can also take immediate steps to strengthen existing privacy rules, for example, empowering consumers to play a greater role in their healthcare by mandating electronic access to their health records. Given the broad array of entities in the e-health arena, the technological changes in the marketplace today, and the prospects for rapid innovation, much of the details of that framework should be worked out through the regulatory process. The challenge for policymakers is to find the right mix of statutory direction, regulatory implementation, and industry best practices to build trust in e-health systems and enable the widespread adoption of health IT.

CENTER FOR DEMOCRACY TECHNOLOGY

FOR MORE INFORMATION

Please contact:
Deven McGraw
Director, CDT's Health Privacy Project
202-637-9800
http://www.cdt.org